

## Malware ili maliciozni softver



Maliciozni softver je softver koji možete instalirati s bilo kojeg medija, među ostalima i s Interneta. *Malware* može imati više funkcija, od prikupljanja osjetljivih informacija, dobivanja pristupa zaraženom sustavu ili mreži, prekidu ili usporavanju računalnih operacija i komunikacija, itd. U današnje vrijeme najčešće se koristi u svrh prikupljanja osjetljivih osobnih, financijskih, korporativnih i ostalih podataka.

Postoji nekoliko vrsta malicioznog softvera:

- 1. Virus** - računalni program koji inficirana neku od pokretačkih datoteka te zahtijeva akciju od korisnika kako bi se aktivirao. Aktivacijom isti izvršava svoj program te dodatno zatražuje druge pokretačke datoteke. Ovisno o vrsti virusa, šteta može biti od jednostavne smetnje do velike štete i gubitka podataka i resursa.
- 2. Crv (Worm)** - je program sličan virusu, koji se aktivno i samostalno širi mrežom u svrhu inficiranja drugih računala. Česti primjer je crv koji se širi emailom i šalje kopije sebe osoba s kojima ste kontaktirali.
- 3. Trojanski konj ili Trojanac** - je malware koji poput pravog trojanskog konja, kamuflira svoju pravu svrhu i vrlo često je prikazan kao koristan softver koji osoba može skinuti s Interneta i instalirati, ne sluteći da se iza toga krije trojanski konj koji se aktivira i odradi svoje skrivene funkcije. A to može biti šteta od brisanja podataka, krađe podataka, otvaranja *backdoor*-a (stražnjih vrata) kroz koje napadač koji stoji iza tog softvera može dobiti puni pristup vašem računalu ili sustavu. Trojanski konj se ne replicira poput virusa i crva.
- 4. Spyware ili špijunski softver** - je softver koji prati vaše aktivnosti, najčešće aktivnosti pregledavanja Interneta u svrhu serviranja pravih reklama za Vas. Naravno isti može imati i puno opasniju svrhu špijunaže.
- 5. Exploit ili iskorištavanje ranjivosti** - isti napada specifične sigurnosne ranjivosti sustava ili produkcijskog softvera.
- 6. Rootkit** - maliciozni softver koji se skriva modificirajući operativni sustav računala i na taj način prikrivajući svoje postojanje. Neki od malicioznih softvera imaju ugrađene sustave obrane od uklanjanja.
- 7. Keylogger** - je maliciozni softver koji, kako mu i ime kaže, služi za bilježenje vašeg korištenja tipkovnice te ponekad slanja slike Vašeg trenutnog ekrana. Njihova najčešća svrha je doći do financijskih informacija i/ili vaših lozinki. Postoje i komercijalne vrste keylogger-a koje se koriste u svrhu nadzora rada djelatnika.
- 8. Dialer** - je softver koji poziva telefonske brojeve s vašeg računala, najčešće preko modema. Vrlo često se radi o pozivima koji nabiju velike telefonske račune, a li isto tako mogu služiti za uspostavu veze između vašeg računala i računala napadača, te prijenos povjerljivih podataka.
- 9. URL Injector** - ima funkciju ubacivanja Internet adrese na mjesto željene adrese, te vas putem vlastitog linka dovede do željene stranice. Isti se vrlo često koristi za stvaranje tzv affiliate (preprodavačkih) linkova.
- 10. Adware** - je najmanje opasan maliciozni softver, ali u isto vrijeme najdosadniji, jer vas vrlo često

obasipa hrpom reklama, koje Vam onemogućuju nesmetan rad.

**11. Ransomware** - je maliciozni softver koji "otme" vaše računalo i traži od Vas otkupninu kako bi isti oslobodio. Poznati slučaj je u kod nas s zaključavanjem računala i porukom MUP-a da imate piratski softver na računalu, te da morate platiti kaznu od 500 kn kako bi Vam se računalo otključalo.

Maliciozni softver se može nalaziti u pokretačkim datotekama, datotekama MS Office-a, PDF-ovima, čak i grafičkim datotekama, skriptama, internet stranicama i sl.

## Kako se zaštititi?

Postoji nekoliko koraka koje je preporučljiv poduzeti kako bi spriječili zarazu Vašeg računala nekim oblikom malicioznog softvera:

1. Instalirajte softver za otkrivanje I uklanjanje malicioznog softver-a (anti-virusni softver, anti-spyware I sl.), vrlo često komercijalni paketi sadrže alate za otkrivanje I uklanjanje svih vrsta malicioznog softvera. Isti redovito nadograđujte najnovijim zapisima o virusima I sl. (najčešće je to automatizirano).
2. Održavajte Vaš operativni sustav I softver koji koristite nadograđen sa najnovijim verzijama i zakrpama (patches, hotfixes).
3. Postanite oprezni prilikom skidanja datoteka s Interneta, otvaranja priloga u Vašoj elektronskoj pošti, pokretanja datoteka na vašem računalu. Sve što vam je sumnjivo, nemojte pokretati.
4. Prilikom instalacije softvera, naročito besplatnog, pažljivo pratite svaki korak instalacije, kako ne bi instalirali *spyware* ili *adware*, te pažljivo pročitajte uvjete korištenja koje morate prihvatiti.

pon, 2013-07-29 13:19 - Darie Marić **Kategorije:** [Sigurnost](#) [1]

**Vote:** 0

No votes yet

**Source URL:** <https://sysportal.carnet.hr./node/1299>

### Links

[1] <https://sysportal.carnet.hr./taxonomy/term/30>